REMARKS

This amendment is responsive to the Final Office Action dated August 11, 2005. No amendments have been made by way of this communication. Claims 1-22 remain pending.

Claim Rejection Under 35 U.S.C. § 103

In the Final Office Action, the Examiner rejected claims 1-21 under 35 U.S.C. 103(a) as being unpatentable over Maritzen (U.S. Pub. No. US 2002/0073042 A1) in view of Bolle et al. (US 6,819,219 B1) and Etzel et al. (US 6,577,734 B1). The Examiner also rejected claim 22 under 35 U.S.C. 103(a) as being unpatentable over Maritzen (U.S. Pub. No. US 2002/0073042 A1) in view of Bolle et al. (US 6,819,219 B1) and Etzel et al. (US 6,577,734 B1) and in further view of Rydbeck et al. (US 6,195,564 B1).

Applicant respectfully traverses the rejection. The Examiner provided no new arguments in rejecting Applicant's claims. The applied references fail to disclose or suggest the inventions defined by Applicant's claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Before addressing the individual claims, Applicant respectfully reminds the Examiner that the present application describes embodiments of a lightweight, wearable personal digital identifier device that provide a high level of security by internally generating a master biometric template and private and public key pairs. Further, the personal digital identifier is configured to prevent transmission of the private key or the master biometric template from the device, thereby providing an increased level of security.

In regard to Bolle, the Examiner overlooked and failed to address the fact that Bolle does not teach or provide motivation to generate the master template on the portable device itself. In fact, nowhere within the disclosure does Bolle describe where the master template is generated. The Examiner continues to incorrectly argue that storing the master template on the portable device is equivalent to generating the master template on the portable device without pointing to any teaching or motivation to do so within the evidentiary record. Applicant's have recognized that possible advantages of locally generating a master template for a biometric on a portable device without requiring the master biometric template be transmitted to the device. Bolle does not recognize nor teach these features, and the teaching and motivation to provide these element of independent claim 1 cannot be plucked from the Applicant's own disclosure.

Similarly, in regard to Etzel, the Examiner overlooked and failed to address the fact that Etzel does not teach or suggest a personal digital identifier device which generates a private key and a public key, as required by independent claims 1, 9 and 17. Etzel teaches that the facility, or centralized video delivery system, performs the function of generating a unique device encryption key. This is in direct contrast to Applicant's claimed invention. Etzel fails to teach or suggest generating private and public keys within a portable, individual subscriber device. Etzel therefore does not teach or provide motivation, when taken alone or in combination with any other provided prior art, for a personal digital identifier device that internally generates both a private key and a public key.

Maritzen fails to overcome these deficiencies. Moreover, in regard to Maritzen, the Examiner overlooked and failed to address the fact that Maritzen does not restricting access to a computer network through a workstation to an authenticated user, as required by independent claim 17. Maritzen teaches that user verification only occurs after the user requests a purchase through the network and workstation. The Examiner has not shown any teaching or motivation within the evidentiary record to duplicate this element of independent claim 17.

Rydbeck also fails to overcome these deficiencies. In addition, in regard to Rydbeck, the Examiner in correctly argued that Rydbeck discloses blanking out a screen when an unidentified wireless device is detected. In fact, the Examiner correctly identified a major deficiency of Rydbeck. The Examiner correctly acknowledged that Rydbeck discloses performing "no action" when an unidentified wireless device is detected. Applicant agrees with the Examiner. However, one or more of Applicant's dependent claims require the specific action of blanking out a screen (i.e., clearing any current display of the screen) when an unidentified wireless device is detected. Moreover, Rydbeck performs no action when an unidentified wireless device is detected merely because the disclosure of Rydbeck provides no capability for detecting an unidentified wireless device. For at least these reasons, Applicant is baffled with respect to the sustained rejection of claim 22.

Claims 1, 9 and 17

As described above, Bolle does not describe or provide motivation to generate the master template on the portable device, as required by independent claim 1. With respect to this argument, the Examiner states "Bolle teaches generating biometric template on a wireless device and storing the generated biometric template only locally in the wireless device to reduce the changes an intruder accessing biometric data" The Examiner then concludes that "In short, biometric template is not generated or stored outside the wireless device." For support, the Examiner cites col. 3, ll. 36-44, which is reproduced below:

> *The present invention provides for a method and a system to wirelessly authenticate a user using a combination of biometrics (e.g., fingerprint) and a locally stored biometric template. By storing the biometric template locally, the current system reduces the chances an intruder can access biometric data.*

As is clear from the plain language reproduced above, Bolle only refers to locally *storing* the biometric template on the device. Many possibilities exist for achieving a locally *stored* biometric of the Bolle system, such as using a central system to generate the biometric template and then transferring the biometric to the device for local storage. Bolle does not teach that the master template is both created and locally stored with the portable device, only that the template is indeed locally stored. The point is that Bolle is silent with respect to the generation aspect of the master template and only refers to the local storage of the template. The Examiner's characterization of col. 3, ll. 36-44, reproduced above, is clearly erroneous based on the plain language of the section.

The Examiner also refers to col. 3, ll. 21-22. This section states that "biometric data stored in databases accessible over a network is susceptible to attacks from intruders." Thus, this section of Bolle only teaches that biometric data should not be permanently stored in a network database. The Examiner concludes that this statement teaches local generation of the template within the portable device itself. However, it is entirely consistent with these cited sections to assume that the biometric data of Bolle may be centrally generated and then programmed into the Bolle device without storing the data permanently within a network database. Bolle does not specifically teach generation of the master template itself within the portable device, thereby avoiding even the transfer of the master template to the biometric device, as claimed by the Applicant. Thus, Bolle cannot anticipate these claim elements.

The Examiner's reasoning with respect to Etzel is similarly flawed. In regard to elements of independent claims 1, 9 and 17, Etzel does not teach or suggest a personal digital identifier device which generates a private key and a public key. As mentioned above, the Examiner must be misinterpreting either the reference of Etzel or the elements of the claims. With respect to Etzel, the Examiner states that "Etzel discloses generating a unique device encryption key and related public key that is never disclosed to another device entity ('externally unknown') and the private and public key in local memory." For support, the Examiner cites Etzel on col. 1, ll. 55-59, reproduced below:

> *We address such needs and advance the pertinent art by providing a facility which implements the secure management of encryption keys. Specifically, in accord with an aspect of the invention, the facility generates a unique device encryption key that is never disclosed externally to another device or entity ("externally unknown") and at least one program encryption key, and then encrypts the program encryption key using the device encryption key and then stores the result in local memory.*

Etzel specifically teaches that the "facility" that generates the unique device encryption key is a central Video On Demand (VOD) system that services multiple subscriber devices. When equating the systems of Applicant's claimed invention and the reference of Etzel, Applicant's personal digital identifier device is similar to the subscriber's device, and the central server of the network is similar to the facility. Thus, neither Etzel nor Bolle, in singularly or in combination, teach or suggest locally a portable device capable of generating a master biometric. Moreover, neither Etzel nor Bolle, in singularly or in combination, teach or suggest a portable device capable of generating both a public key and a private key.

Applicant's claims specifically require that the personal digital identifier device generates the private and the public key. Further, the Applicant's description states that "the PDI device itself generates and internally stores the user biometric templates and one or more public and private keys (emphasis added)."[1] Since the reference of Etzel does not provide a teaching or a motivation for the generation of keys to occur at the subscriber's device, it would not be obvious to someone of ordinary skill in the art to generate the private key and the public key at the personal digital identifier device. In fact, any modification of Bolle in view of Etzel would result in a central system (i.e., a central facility) that generates encryption keys for all of the portable

[1] Application, Page 12, Lines 25-30.

devices and fails to share them with the devices, thereby failing to achieve Applicant's claims as suggested by the Examiner.

In regard to independent claim 17, Maritzen fails to teach or suggest restricting access to a computer network through a workstation to an authenticated user. To the contrary, Maritzen allows access to the workstation and computer network at any time. Authentication of the user is only required once the user desires to purchase an item from a vendor through the network. Maritzen states:

> *"When the personal POS terminal receives the transaction request, it communicates with the transaction device, asking the transaction device to validate the user..."*[2]

As this description from Maritzen shows, the user has already accessed the personal POS terminal by requesting the transaction.

The user in Maritzen has access to the network without being validated. Without already having access to the computer network to browse the items offered for sale by the vendor, the user would not be able to select an item to buy. Further, by allowing the user to access the network without authentication or validation, the reference of Maritzen fails to provide motivation for requiring authentication before allowing network or workstation access.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's independent claims 1, 9 and 17 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

Claims 4 and 14

Dependent claims 4 and 14 are patentable for at least the reasons stated above with respect to independent claim 1 and 9 from which they depend.

Moreover, the Examiner failed to elaborate on the statement that Etzel teaches data stored in the storage by itself is not identifiable by a user or provide relevant prior art. The Examiner is either misinterpreting the reference of Etzel or the claims. The cited description pointed to by the Examiner only refers to a facility securely maintaining keys for encrypting video programs. Since the video programs are not assigned or associated to any user, they do not contain sensitive data from a user. Therefore, the video programs, or any other data, would not be identifiable of a

[2] Maritzen, Page 15, Paragraph 0206.

said user in any aspect of the Etzel system. Applicant is confused by the application of the Etzel reference in rejecting claims 4 and 14. The Examiner is using prior art that is not related to the elements of the claims, so there is no motivation to protect the identity of user data when the data does not contain any information related to the user.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims 4 and 14 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

Claims 15 and 20

Dependent claims 15 and 20 are patentable for at least the reasons stated above with respect to independent claim 9 and 17 from which they depend.

In regard to claim 15, Maritzen fails to suggest a security system wherein said network storage includes data identifiable of said user for display on a screen of said workstation when said user's personal identification device is located within said envelope. The Examiner must be misinterpreting either the reference of Maritzen or the claimed invention. Maritzen discloses that secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized.[3] However, purchased content is not identifiable of a user. For example, if the user utilized the invention of Maritzen to buy and download a digital music track, that digital music track is not identifiable of the user. It is simply distributed content.

Moreover, Maritzen never describes or provides motivation for an envelope in which a personal identification device is located. Maritzen only states that "the digital wallet transmits a signal to the PC or DTV."[4] There is no suggestion or motivation for an envelope in which the digital wallet may transit the signal to the PC or DTV. Furthermore, Maritzen suggests that signal transmission may occur at will, no matter where the digital wallet is in relation to any other device within the system. There is no limitation on the transmitting capabilities of the digital wallet. Therefore, the reference of Maritzen provides no motivation or desire to someone of ordinary skill in the art to duplicate the elements of claims 15 or 20.

[3] Maritzen, Page 16, Paragraph 0210

[4] Maritzen, Page 15, Paragraph 0202.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims 15 and 20 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

Claim 22

Dependent claim 22 is patentable for at least the reasons stated above with respect to independent claim 17 from which it depends.

The Examiner has correctly pointed to a major deficiency within the Rydbeck reference with respect to the elements of claim 22. The Examiner stated that Rydbeck discloses performing no action when an unidentified wireless device is detected. Applicant is confused as to why the Examiner continues to reject claim 22 when the Examiner specifically acknowledged a significant difference between Rydbeck and the claimed invention. In contrast, claim 22 requires performing the action of blanking out a screen when an unidentified wireless device is detected. Since the action performed in claim 22 is the opposite of Rydbeck teaching of no action being performed, Rydbeck provides no motivation for someone of ordinary skill in the art to perform any action upon detecting an unidentified wireless device.

Moreover, the reference of Rydbeck fails to teach or suggest the detection of an unidentified wireless device. The laptop computer 100 in Rydbeck is only capable of detecting the one associated phone 300 and is not described as being able to detect another phone 300 or an unidentified phone 300. Rydbeck states, "laptop computer 100 checks for a page signal from the wireless phone 300."[5] Therefore, the applied reference fails to provide motivation to someone of ordinary skill in the art to detect other wireless devices.

Further, Rydbeck never discusses the screen of a workstation being blanked out. The system of claim 22 includes a policy manager component which may direct that the screen of a workstation be blanked out when a new personal digital identifier device moves to a location within said envelope. Rydbeck only describes laptop 100 staying in standby mode. Rydbeck never teaches that a screen is blanked out at any point within the disclosure.

The Examiner must point to motivation within the evidentiary record to incorporate the features of Applicant's claim 22 into the reference of Rydbeck and other applied art. The applied

[5] Rydbeck, Col. 6, Lines 48-49.

prior art provides no such motivation. Instead, it appears that the Examiner is merely pulling motivation directly from Applicant's disclosure.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claim 22 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:
October 11, 2005
SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

By:
Kent J. Sieffert
Name: Kent J. Sieffert
Reg. No.: 41,312